Tab C

Preliminary Research and Development Roadmap for Protecting and Assuring the Information and Communications Infrastructure*

* This document is one component of a longer report entitled *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office. Washington, D.C. July 1998). For more information, please see <URL:http://www.ciao.gov/>.

Contents

Contents (Cont.)

Tables

Section 1
Introduction

The U.S. information and communications infrastructure (ICI) is integral to our nation's security and economic competitiveness. Experts agree that this infrastructure is fragile and cannot defend or heal itself adequately. Without continual vigilance and renewed efforts to bolster security, the ICI would degrade or fail in the event of an attack or disaster.

This report expands on the 1997 study performed as part of the work by the President's Commission on Critical Infrastructure Protection. In their report, the Commission recommended a series of research and development (R&D) topics and their priorities to provide a greater level of assurance for critical infrastructures they had identified. The Commission studied eight critical infrastructures: banking and finance, electric power, emergency services, government services, information and communications, oil and gas production and storage, transportation, and water supply.

This effort expands on the ICI baseline report. It provides a technology R&D[1] "roadmap" that suggests a research agenda to develop methods required to improve protection of the ICI. This effort is the product of a working group composed of representatives from national laboratories, government agencies, industry, and academia.

1.1 Scope of the Infrastructure

The ICI consists of three primary layers. The first layer (physical layer) is an underlying "link" that moves data from point to point (e.g., satellites, copper wire, optical fibers, wireless transmissions). The second layer is a network and transport layer that deals with addressing, routing, and data transport services. The third layer consists of the computing systems and applications that generate, manipulate, store, display, or control the ICI, for example, by using information and facilitating human collaboration and creative activities. The combination of these three layers provides a full spectrum of communication, computation, control, information, and human collaboration systems that is critical to all aspects of society.

The ICI is closely coupled to the other infrastructures studied by the Commission. Because of the strong interdependencies among the ICI and the other infrastructures, a break in the ICI can affect other infrastructures, such as banking and finance. In addition, the ICI depends on other infrastructures, such as the electric power infrastructure.

---

1 Throughout this report, the words "research" and "development" are used synonymously.

For their link layer, most wide-area data networks use "public-switched networks," the system of control centers, communication lines, and circuit switches maintained and operated by the telecommunications industry. Internet technology differs from the public-switched network primarily because all communication is accomplished by breaking the data streams that provide the services mentioned above into "packets" that are independently routed through an inter-network. The Internet protocol routing element of the ICI has a different set of vulnerabilities than the switched network, which also requires research in routing security.

1.2 Characterization of the Infrastructure

1.2.1 Rapid Evolutionary Growth and Change

The ICI systems have undergone dramatic changes in the last decade. Once dominated by AT&T, the communications industry is now represented by numerous players in both the local and long distance markets. In addition to providing communications services, many of these companies are beginning to offer other services, such as Internet connectivity.

In the area of communications, wire-based telephony is rapidly being supplemented by wireless systems. The introduction of affordable satellite telephone systems means that soon anyone can phone any point in the world. In addition, most U.S. military communications depend largely on commercial systems.

In just a few years, the Internet has evolved from a low-bandwidth network used by the military and the scientific community to a system that literally anyone can access. It is hard to find an organization that does not have an Internet home page, and e-mail rapidly is becoming the preferred form of communication in many organizations.

1.2.2 Interdependencies

The boundaries between the individual elements in the ICI have become less distinct. Every component of every layer in the ICI relies on computer control. Internet communication is being used increasingly to control and manage the components of the layers below the Internet (i.e., the public-switched network, routing infrastructure of the Internet). Many modern computer applications use Internet technology for communication, whether through the global and public Internet, or in private (isolated) corporate Internets (sometimes called "Intranets"). Software is being developed that automatically connects users to the Internet; also, numerous packages are available to assist the user in building Web sites. With this pervasive assimilation of the Internet into the ICI comes the reality that geographic boundaries are becoming less meaningful. With this geographic transparency in the Internet, a cyber attack could come from anywhere. Because of the close interaction among computers and the other infrastructures, all infrastructures are vulnerable to a cyber or a direct physical attack. For example, the

viability of remote control systems, such as the electric power system's Supervisory Control and Data Acquisition (SCADA) systems, depends on the ICI.

1.2.3 Regulatory State

Federal regulation of wireline and wireless communication of voice, data, and image signals within the United States is authorized by the Communications Act of 1934 (the Act),[2] as amended by the Telecommunications Act of 1996. The Act established the Federal Communications Commission (FCC), within the U.S. Department of Commerce, as the body to execute and enforce its provisions. The FCC is now an independent agency.

With regard to national infrastructure policy, however, the FCC is neither the sole developer nor the only purveyor. The National Telecommunications and Information Administration (NTIA), created recently within the U.S. Department of Commerce, has, through its Office of Policy Analysis and Development, the role of "principal advisor to the President on telecommunications policies."[3] As one of its primary policy functions, the NTIA was directed by Congress to foster "...national safety and security, economic prosperity, and the delivery of critical social services through telecommunications."[4] The NTIA has filed numerous replies concerning matters docketed before the FCC to express the administration's desires with regard to deregulating the industry, in particular the assurance of universal access to telecommunications service at affordable rates (NTIA 1996).

In addition to the federal presence, all 50 states have some form of regulatory body that addresses telecommunications, generally a public utility commission or a subpart thereof. For the most part, state agencies are concerned only with facility siting, equipment siting, and rate-setting matters, but a growing number are addressing access and continuity of service issues (Q.V. 1995–1996). They focus primarily on promoting and accommodating commerce, while ensuring the most democratic distribution of service economically permissible.

1.3 Issues and Trends

The explosive growth of wireless communications characterizes the rapid technological development that has occurred in the ICI. New area codes are being created at a rapid pace, and the U.S. telecommunications industry is beginning to face the issue

---

2 47 USC - *Telegraphs, Telephones, and Radiotelegraphs.*

3 47 USC §901.(b)(6); and U.S. Department of Commerce Word Wide Web Home Page, National Telecommunications and Information Administration, Office of Policy Analysis and Development (http://www.ntia.doc.gov/opadhome/opadhome.html).

4 47 USC §901.(c).

that demand is outpacing supply with respect to the current 10-digit phone number structure.

The use of the Internet is expanding faster than society can cope with it. Particularly problematic are the reach and the speed of information transmission via the Internet. With the Internet, information can be disseminated around the world in seconds. Increasingly, telephone service is being provided over the Internet, and this trend significantly affects the reliability and security of Internet technology.

1.3.1 Managing the Internet

In terms of transferring or sharing information, the Internet is difficult to categorize because it combines software and communications protocols. From its beginning as a network developed and supported by the U.S. government, it is today an international communications resource. Some groups believe the Internet should be totally unregulated and that anything posted on it should be free for anyone to use.

1.3.2 Establishing a Legal Basis for Cyberspace

Legal theorists are struggling with how to develop and apply laws for the Internet. Do laws developed for print or broadcast media apply to the Internet? How can electronic documents be protected by copyright and watermarks? A recent Supreme Court ruling, which overturned an attempt to regulate content on the Internet, illustrates that the legal status is quite unclear.

The ability to exchange data and information widely on the Internet also has provided an entry point for computer viruses and other malicious code. Until recently, few laws governed “cyber” attacks against computer systems, and existing laws were not well enforced.

As the Internet becomes a medium for commerce, a number of issues have emerged. For example, the security of Internet electronic transactions is a subject of active debate. Even with the introduction of encryption, the perception is that Internet commerce is less secure than conventional commerce. Another issue is liability; that is, who is responsible if credit card numbers are stolen — the Internet service provider or the Internet commerce provider?

1.3.3 Developing Critical Technologies Offshore

Many critical technologies and security products are developed at non-U.S. locations or by companies that are wholly or partly foreign owned. Moreover, many software development efforts are exported to other countries that have either cheaper labor costs or a greater abundance of available programmers. A concern is that these offshore developments may result in the insertion of software “back doors” or hidden “sleeper” code that could go undetected and be accessed by a hostile agent.

1.3.4 Collecting Data and Ensuring Privacy, Dissemination, and Protection

More data are being collected on individuals and organizations and are being "mined" and warehoused to create profiles for marketing and other purposes. These data are sold, in most cases, without the knowledge of those profiled in the databases. Internet providers also can and do track usage patterns, often without the knowledge or consent of the user. While this practice is perfectly legal, concern is increasing in regard to personal or organizational invasion of privacy.

Section 2
Threats and Vulnerabilities

It is impossible to build a perfectly secure ICI, so the goal is to design and build cost-effective systems with the degree of protection consistent with the needs of users and to emphasize continual improvement. The threats to the ICI can come from a variety of sources, such as deliberate attacks (cyber or physical) by insiders or outsiders, natural disasters, simple accidents, or failures in poorly designed or outmoded equipment. A recent series of hacker attacks against U.S. Department of Defense (DoD) computer systems vividly demonstrates the reality of these threats.

Although the possibility of cyber attack has received increased attention (*Defense News* 1998; *The Washington Post* 1998), the threat to the ICI from physical attack must not be excluded. Satellites and ground-station equipment are highly vulnerable to a physical attack and interference, and, if they should occur, the impact could be felt on a global scale. Many of the recent serious disruptions in the ICI have occurred through physical means, such as cable breaks, other accidents, or natural disaster.

Section 3
R&D Topics and Activities

Thirteen R&D needs in the information and communications infrastructure are prioritized as "most important," "very important," or "important." These needs are further categorized into three primary research areas: (1) risks, threats, and vulnerabilities; (2) intruder and incident detection response, and recovery; and (3) engineering high-confidence infrastructure.[5] In addition to these areas, modeling and simulation tools are needed that cross all of these areas. The topics presented are in addition to any of the basic and applied research being performed in the classified communities. The R&D activities outlined in this report need to leverage, complement, and integrate with the research underway in the various government agencies and departments, as well as the private sector. These research results may also require protection. Government-funded research should not duplicate or reinvent the progress driven by market forces; rather, it should focus on areas not addressed sufficiently by the private sector, long-term research, and specialized technology required by the government.

It is expected that strong synergistic relationships will form among these areas, with results from one area driving research in others. These research topics are interrelated in a dynamic and nonlinear fashion, which raises the complexity of a research plan. The resulting research will be used to improve the security and protection in legacy and future systems and technologies.

3.1 Risks, Threats, and Vulnerabilities

The objective of this area is to develop the essential information, tools, and procedures for identifying, analyzing, and continuously managing the risks inherent to the ICI and those imposed by outside forces. Risk management is used to analyze the relationships among five critical components:

- Assets — the resources or objects of value to be protected;
- Threats — the sources or causative agents that can harm the system or cause loss;
- Vulnerabilities — the "windows of opportunity" through which a threat can materialize;
- Losses — the direct or transient effects on users of the system, resulting from something possessing or representing value being removed, devalued, denied, or

[5] A significant reference for this section is a report by Mayfield (1998).

otherwise exploited, such as lost information, degraded computational or communications resources, falsified data, loss of life, or loss of confidence in the system; and

- Safeguards — the physical, administrative, and technical controls designed to provide protection and reduce vulnerability.

Risk management ultimately determines what investments to make to provide a specified level of protection and what cost one may be willing to accept in the form of potential losses and putting in place the necessary contingency plans, procedures, and resources to mitigate the effects of such losses.

The anticipated products from this research area include the collection of data and information for characterizing and analyzing risks, threats, and vulnerabilities; the development of procedures to manage such information; the development of software tools; and the advancement of key theoretical areas. Specific areas that require support for R&D are described in the following subsections.

3.1.1 Vulnerability Detection and Analysis

Description

The first objective for this research is to identify, collect, organize, and disseminate system, network, and infrastructure vulnerability information. The second objective is the development of applied technologies and methodologies to avoid, reduce, or eliminate vulnerabilities during the development of hardware and software products and their integration into systems. This research would result in (1) a lexicon of threat and vulnerability information, (2) methodologies and information databases on vulnerability and attack taxonomies, and (3) technologies and methodologies to analyze vulnerabilities. Short-term results could be expected as information databases are assembled and shared, but a continuing research investment would be required. Specific areas of research are described in the following subsections.

Develop Threat and Vulnerability Lexicon. A lexicon of terms needs to be developed so that data can be precisely defined and collected. This effort should extend the earlier works on information security performed by the National Security Agency Information System Security Organization,[6] the Federal Bureau of Investigation (FBI), and DoD. The requirement for a lexicon spans all of the infrastructures being studied. It is recommended that this task be pursued first, and that a system be considered that is similar to the one used by the FBI for defining and reporting crime statistics. A lexicon, and a subsequent vulnerability and attack taxonomy for both cyber and physical attacks,

6 See, for example, ISSO's *Unified INFOSEC Glossary*, V 2.0, 1996.

could be useful for many purposes, such as incident handling, crime statistics reporting, intrusion detection, and vulnerability analysis.

Develop Vulnerability and Attack Taxonomies. Research is required to develop vulnerability and attack classification taxonomies (e.g., distributed coordinated attacks against a single target, a single attack against many targets, and distributed coordinated attacks against multiple targets). This research is required to support the prediction and testing of new vulnerabilities. Ideally, it would enable the development of tools for testing vulnerabilities and methodologies for analyzing programs and systems in a systematic fashion. The problem of classification is subtle because of the interaction of the level of abstraction and the point of view within which the vulnerability occurs. Such research would lead to the development of a database of vulnerabilities useful to other areas of security.

Develop Tools to Analyze Vulnerabilities. Research is required to develop tools and techniques to support the identification of, interdependencies among, and understanding of the vulnerabilities in systems and networks. Examples of tools needed are configuration checkers, functional testers, attack and penetration analyzers, topology mapping software, visualization tools, and modeling and simulation frameworks. Additional research is required to develop a new generation of automated technology that analyzes; provides an alert; or avoids, reduces, or eliminates vulnerabilities during the development or integration of hardware products. These technologies could employ intelligent agents, for example, that would operate on a semi- or fully autonomous basis.

Automate Vulnerability Analysis Technologies. Research is required to support the development of automated technologies to analyze, provide an alert about, avoid, reduce, or eliminate vulnerabilities while developing or integrating hardware and software products.

Study Satellite and Wireless Communications. Satellite and wireless communication systems have unique vulnerabilities that require an end-to-end study. Although these systems share many of the threats and vulnerabilities of wire-based systems, unique aspects for protecting these systems are evident. The physical aspects of security include protecting the ground stations and transmission disks. Satellites are subject to jamming, interception, collision, interference (regarding the signals and the control systems of these satellites), as well as malfunctions, electromagnetic interference, and environmental impacts (e.g., solar flares). The increasing reliance of military communications on commercial satellites requires adequate protection for these systems.

In addition, satellite services, such as the Global Positioning System, provide both location information (on which the transportation infrastructure depends) and essentially a global clock (on which cellular phone services depend). These services are international in scope, and the protection of these assets requires agreements, treaties, and enforcement at an international level.

Goals and Challenges

The goal for this R&D topic is to produce technologies and methodologies to detect and analyze vulnerabilities in integrated systems and networks efficiently and cost-effectively.

The challenge is to have procedures and tools for collecting and disseminating vulnerability data in place at the national level and, it is hoped, at the international level.

Rationale for the Research and Desired Results

The rationale is, that to apply protective measures, one must be able to identify where the vulnerabilities are in the ICI and how they might be exploited by an attacker.

Timeframe and Resource Requirements

The estimated total investment over this time period is $330 million.[7] The proposed commitment is $90 million in 2000, $90 million between 2001 and 2005, and $150 million between 2006 and 2010.

3.1.2 Valuation of Information

Description

Research is required to develop tools and methodologies to assist information owners in determining how to value their holdings and determine what level of protection is appropriate. A means for determining the value of information also would be useful in risk management, the determination of critical assets, and the insurance industry.

In addition, tools and methodologies are required to evaluate the effect of aggregated information. This effort is important especially because by using data-mining techniques, individuals or entities can collect data from multiple sources to develop a "picture" or "report" that otherwise would be considered sensitive or confidential.

Goals and Challenges

The goals and challenges are to provide efficient and easy-to-use tools and procedures for valuing information and determining the appropriate level of protection.

[7] All years referenced in this document are fiscal years.

Rationale for the Research and Desired Results

The requirement for these tools is critical because if service is interrupted, the impacts can be distributed widely and are potentially life-threatening. Therefore, a form of triage assessment will be required to determine what information and data assets are given priority in terms of protection and recovery. Because the value of information may be linked to time and context, an assurance level approach may be appropriate. Such an approach makes it possible to use the importance or criticality of information to the system function to determine the level of assurance for the system.

Timeframe and Resource Requirements

The timeframe for this activity extends to 2010 and beyond. The total estimated investment over this period is $110 million. The proposed commitment is $30 million in 2000, $30 million between 2001 and 2005, and $50 million between 2006 and 2010.

3.1.3 Risk Analysis

Description

Conventional risk analysis consists of surveying the components of a system or network, as well as the users, to determine the exposure of valued resources to loss, damage, or denial. Such an analysis often is performed manually, although some commercial off-the-shelf tools are available to automate the collection and analysis of the survey information. These analyses are also typically done on a periodic basis, such as annually. Although sound analyses of risk are often performed during these annual security exercises, risk management needs to be performed on a continuous basis, especially if changes are made to the system or network (e.g., changes in equipment, software, or procedures). Automated tools and technologies are required that detect new components in systems and networks and that then can assess the vulnerabilities in the modified system. Metrics need to be developed for evaluating security technologies, in particular, tools to evaluate the cost-benefit of implementing changes in systems. Specific research topics related to the development of automated risk management and cost-benefit tools and metrics are discussed in the following subsections.

Automated Risk Management. Automated tools and techniques are needed to support risk management. The desired tools need to be able to detect automatically when new software or hardware is added to the system or network. These tools would analyze the new component and present an analysis of known or postulated threats that could exploit discovered vulnerabilities in the new software or hardware component, a prediction of the likely exploitation path, and an assessment of the potential consequences. Research is needed in foundational techniques to support the development of such automated tools across systems, networks, and infrastructures.

Risk Management Metrics. Metrics for evaluating security technologies need to be developed. Measures of effectiveness and performance must be defined to enable managers to evaluate and compare security technologies.

Cost-benefit Analysis. Tools and techniques are needed to enable developers and integrators to estimate the investment and performance costs of implementing security technologies and/or procedures. These tools and techniques must be able to incorporate such critical concepts as "trust," the value of information and system resources, timeliness and responsiveness, ease of use, cost of ownership, and potential liabilities. Trade-off algorithms and associated metrics used to balance desired cost-performance attributes appropriately must be developed to provide the foundation for such tools. The development of such algorithms and metrics likely would require extensive experimentation, that is, similar to what has been done in hardware and operating system performance analyses.

Goals and Challenges

The goals and challenges are to provide efficient, easy-to-use tools and methodologies for analyzing and measuring risk in evolving environments and to perform cost-benefit trade-off analyses.

Rationale for the Research and Desired Results

The rationale is as follows: given that risk cannot be completely eliminated, managers and implementers need to be able to reduce risk to acceptable levels and to evaluate the trade-offs between risk reduction and cost.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010. The estimated investment over this period totals $200 million. The proposed commitment is $75 million in 2000, $75 million between 2001 and 2005, and $50 million between 2006 and 2010.

3.1.4 Characterization and Notification of Threats

Description

Threats to the ICI can come essentially from any point in the world. However, the implication of a specific threat varies with the targeted infrastructure element (e.g., individual, corporate, national, international) and the objective of the attack (e.g., mischief, crime, espionage, terrorism, information warfare). This effort is primarily a data collection and analysis, which can effectively leverage existing intelligence databases, with respect to the threats to the ICI. Specifically, data would be collected to assist in characterizing threats in terms of motivation and origin and to develop tools and

technology that would profile attackers and pinpoint where the attacks are coming from. Specific research areas under this topic are described in the subsections below.

Characterize Threats by Motivation and Origin. Limited data are available for characterizing threats on the ICI. Research is required to characterize and identify threats in terms of their motivation and origins. This research is required to develop tools and procedures for identifying potential threats in existing and emerging technologies.

Profile Potential Attackers. Data of relevance for determining what constitutes a potential ICI attacker are limited. Research is required to develop profiles of potential attackers that incorporate such factors as motivations, origins, and capabilities. Threat identification and characterization should include attack methods and prerequisites. It is necessary to understand the differences and similarities between threats from system "insiders" (i.e., system administrators, privileged users, flawed applications) and threats from "outsiders" (i.e., hackers, viruses, intruder-inserted malicious code).

Insiders are a very significant part of the threat spectrum; an estimated 75% to 80% of problems are caused by those who are familiar with the vulnerabilities of systems and the locations of critical system data. Advanced tools are required to monitor the usage patterns of insiders and flag access behaviors that fall outside normal patterns. This research would need to be performed for both individual and organized attackers (e.g., groups or countries). It would provide a foundation for developing tools and procedures to help identify potential threats to existing and emerging infrastructures.

Developing profiles of outsiders is especially difficult because of the anonymity that is possible with the Internet. Fundamental research in human behavior and psychology is required to develop approaches to analyze threat potential on the basis of how one accesses and uses ICI elements.

Pinpoint the Origin of Attacks. Pinpointing the source of attack (physical or cyber) is critical in knowing where to apply defensive measures and where to trace back to search for the attacker. (The discussion in Section 3.2.1 is related to identifying the source of cyber attacks.) Funding is required to enable existing infrastructure managers to analyze carrier interconnections and operations to help pinpoint the origin of attacks. These analyses would allow development of cooperative response strategies. Properly applied forensics and data sanitization procedures also would need to be developed to enable necessary data to be collected and appropriately shared for use in isolating and prosecuting attackers. The latter is important because the interconnectedness in networks promotes the loss of accountability and ability to trace sources of attacks.

Funding in this area would yield both short- and long-term benefits. In addition, a continuing research effort would be required as new technologies are developed and introduced into the ICI. The primary benefits from this research would be sharable data and information and the procedures and tools for collecting, analyzing, and disseminating the data and information.

Goals and Challenges

The goal of this effort is to collect, analyze, and distribute timely and accurate data on the threats to the ICI. Tools and technology are needed to analyze the data to profile both insider and outsider attackers, and to trace the attack across interconnecting networks to the point of origin.

Rationale for the Research and Desired Results

The rationale for this topic is to construct defenses against threats to the ICI, and one must first identify and characterize those threats.

Timeframe and Resource Requirements

By 2010, a formal system for collecting, characterizing, and disseminating threat data should be in place at the national and the international level. It is estimated that a total federal investment of about $95 million is required through 2010. The estimated commitment requires $25 million in 2000, $30 million between 2001 and 2005, and $40 million between 2006 and 2010.[8]

3.2 Intrusion and Incident Detection, Response, and Recovery

The objective of this research area is to develop tools and procedures to detect, respond to, and recover from incidents, losses in service, or attacks. Incident detection is different from intrusion detection. With incident detection, someone or something causes an anomaly or problem, while with intrusion detection, someone or something is assumed to be "looking around," gaining unauthorized access to information or preparing to attack with the intent to damage, disrupt, deny, or destroy.

3.2.1 Intrusion and Incident Detection and Warning

Description

Detecting incidents is not necessarily a straightforward activity. The development of intrusion detection systems is still in its infancy. Also, the results of an incident may not necessarily manifest themselves at the time of the incident. For example, data may be corrupted, but the fact that they are corrupted may not be known until they are used. Once an incident has been detected, the elements in a system or network may be compromised, and alternative systems may need to be used to send a warning. Intrusion detection systems also need to be protected from attack, as these systems have vulnerabilities, too.

[8] The funding estimates given for the 2006 to 2010 timeframe probably would change as a result of developments during the 2001 to 2005 period.

The objective of this research is to develop tools and procedures to identify and report the precursors to an attack, or an actual attack, on the ICI. Tools need to be developed that are scalable to large systems and networks and that can respond to different attack strategies (Section 3.1.4). In the short term, manual procedures may be required to provide communications between incident handling teams. In the long term, the goal is to develop automated indications and warning systems.

The effort would focus on the development of metrics for evaluating false-alarm rates, strategy-based intrusion detection technologies, tools and technologies for use on high-speed networks, scalable intrusion detection systems, and tools to trace intrusions to their sources.

False-alarm Metrics. Existing intrusion detection systems (IDSs) suffer from high false-alarm rates and unknown, but probably very high, false-negative rates. The goal of this R&D is not to determine the values for "acceptable" false-alarm rates, but to develop standardized algorithmic metrics that can evaluate IDSs so implementers can judge the "quality" or "fitness" of an IDS and then compare systems.

Strategy-based Intrusion Detection. Intrusion detection technologies need to be developed on the basis of different analysis strategies. Examples of new approaches include the following:

- Detecting deviations from the expected behavior of a program or service;
- Using data fusion and data mining tools;
- Analyzing patterns of attack (e.g., signature patterns) to detect denial of service;
- Analyzing "anomalous" or uncharacteristic user behavior; and
- Detecting deviations from the policy-based mandates on the functioning and operation of the network.

High-speed Network Intrusion Detection. Intrusion detection technologies need to be developed for use with high-speed networks. When the network speed increases, a simple or minor security attack can cause problems that can be propagated through a system rapidly. However, the key issue is not the rate at which the problem spreads, but rather the difficulty of performing detection activities with the increasingly faster data rates that are becoming available.

Scalable Intrusion Detection. Components of an information and communications network can be numerous and geographically dispersed. Intrusion detection technologies need to be developed that are scalable to systems and networks at a national level, with thousands of potential penetration nodes that could be geographically diverse.

Trace Back. The ability to trace a cyber intrusion rapidly back to its source is critical in stopping attacks. If the trace can be done rapidly and in a stealthy fashion, it may be possible to catch the attacker. Therefore, technologies and procedures are needed to identify, analyze, isolate, and trace back to their sources any actual or suspected intrusions. These tools would need to produce supporting forensic data that could provide credible evidence in courts of law.

Goals and Challenges

The goal is to develop efficient, cost-effective, real-time tools for intrusion and incident detection and warning. These tools are needed at a national level to integrate information from distributed sources; taken together, such information may warn people of an impending attack.

Rationale for the Research and Desired Results

The rationale for this research is that disruptions in the ICI can have far-reaching effects, including the creation of life-threatening situations. Therefore, technologies and tools are required to detect intrusions and incidents and to send out warnings rapidly and efficiently.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010. The total estimated investment over this time period is $330 million. The proposed commitment is $90 million in 2000, $90 million between 2001 and 2005, and $150 million between 2006 and 2010.

3.2.2 Response, Recovery, and Reconstitution

Description

Once an attack or incident has been detected, a system or network is restored to full working order by using a three-phase process. The first phase is response — deciding what must be done, in what order, and with what resources. The second phase is recovery — repairing the damage and returning to a degraded mode or full operational capability. The last phase is reconstitution – replacing resources that have been completely destroyed or are beyond repair. The objective of this research is to develop methodologies to contain, stop, or eject intruders and to mitigate damage or restore information processing services in the event of attack or disaster. Specifically, the research would focus on developing tools and methodologies to make rapid assessments of damage from an attack or break in the infrastructure, improved technologies to reject and contain intruders, and more timely and effective network recovery or reconstitution.

Response Assessment. Because response must be immediate, there is an urgent need to develop procedures and tools to perform a triage assessment of the extent of damage from an incident or attack. The assessment methodology would probably follow medical approaches and focus on establishing priorities for applying recovery resources. This research would focus on how to determine what infrastructure elements are "dead," or nonrecoverable, and how to eliminate or isolate them without damaging the rest of the system or network. Tools are needed for self-healing, self-correcting, and self-diagnosis on networks and systems. In the short term, manual procedures may be required, but in the long term, automated tools are desired.

Intrusion Rejection. Once an intrusion has been detected, it must be eliminated as a threat. Therefore, procedures and technologies are required to reject, eject, and/or contain intruders at all stages of attacks or threats to the infrastructure, natural or deliberate. In the short term, manual procedures may be required to provide real-time corrective or adaptive response, but in the long term, automated tools are desired.

Network or System Recovery and Reconstitution. Tools and procedures are needed to recover and reconstitute a network or system in the event of a break. Recovery is best carried out hierarchically, starting at the lowest level and attempting to recover to a known state. A level is restored to a consistent state before recovery is attempted at the next higher level. The tools and procedures used to facilitate recovery and reconstitution would have to identify all affected elements (hardware, software, and data/information) and provide the ordering and procedures necessary for recovery in an orderly fashion. To provide information that could be trusted, these systems would have to be isolated or "hardened" to attack.

Goals and Challenges

The goals and challenges are to reduce the times needed for, and increase the effectiveness of, responding, recovering, and reconstituting systems and/or networks if a disruption occurs.

Rationale for the Research and Desired Results

The rationale for this research is that breaks in the ICI can result in serious, and potentially life-threatening, impacts on society, organizations, and individuals. Reduced time and increased effectiveness to respond and recover are critical for restoring the systems and networks.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010. The estimated investment totals $300 million. The proposed commitment is $95 million in 2000, $105 million between 2001 and 2005, and $100 million between 2006 and 2010.

3.3 Engineering High-confidence Infrastructures

So far, research has focused on knowing where threats and vulnerabilities will be and how to respond to them. Now the focus shifts to making the ICI and other dependent infrastructures more resistant to attack. This research focuses on developing the tools and procedures for building the ICI with minimal vulnerabilities. The resulting products would be applicable for retrofitting legacy systems, as well as for applying to emerging technologies.

3.3.1 Security Architectures

Description

The objective of this research is to organize security components and services to provide confidentiality, integrity, and availability for information and communication systems. For example, research conducted under this topic would examine areas such as the following:

- Interoperability among security components,
- Policies for security implementation in emerging technologies,
- Advanced firewall technologies,
- Adaptive systems,
- Packet-switching technologies,
- Secure operating systems for the Internet and automated distribution of patches and information related to security upgrades,
- Scalability and optimization of security architectures, and
- Vulnerabilities in remote control systems such as SCADA systems.

Interoperability among Security Components. When networks and systems become interconnected, security features in one system may be in conflict with security features in another. This incompatibility can be especially true if systems, such as communications systems, span national boundaries, and different standards or approaches are used. Therefore, architectures need to be defined with protection protocols and data exchange interfaces to allow interoperation of security components.

Policies for Security Implementation in Emerging Technologies. It is difficult to predict what technologies will be a part of future ICIs. Therefore, it is a pressing need to develop policies for implementing protection measures within emerging

technologies and to focus on engineering security into the technologies as early as possible. In addition, a formal notation, or policy language, must be developed to capture policy for reasoning purposes.

Advanced Firewall Technologies. Firewalls are often the first line of defense in computer systems and networks. As attack technologies and strategies become more sophisticated, firewall technology must advance as well. A recent article in a trade magazine indicated that the quality of commercial firewall products is unsatisfactory and that many of the packages can be easily penetrated (*Internet Week* 1998). The proper configuration of firewalls is important, and tools are needed to assist system administrators. Advanced firewalls are beginning to include intrusion detection and encryption technologies.

Adaptive Systems. Advanced systems and networks are needed. These need to be adaptive and capable of reacting dynamically to changes in the security and reliability environment.

Packet-switching Technologies. Research is required to develop a packet-switching technology (also known as "Internet switching architecture") for supporting isolation of one-to-one, one-to-many, and many-to-many communication flows with respect to bandwidth, throughput, rate of data loss, and security (data encryption and origin-destination encryption).

Secure Operating Systems for the Internet. Considerable activity surrounds the development of the "next generation" Internet. Secure and reliable operating systems are needed for the Internet nodes of the present and future systems.

Automated Distribution of Security Patches. Often the weak link in a security system is the inability to distribute and implement security notices and patches fast enough. Therefore, a protocol is needed for automated distribution of security patches and notices that can operate even under potentially degraded circumstances.

Scalable Security Architectures. Scalable and robust security architectures are needed to meet the need for larger environments. Work in this area would leverage off results from the development of attack taxonomies.

Optimized Security Architectures. The performance of systems and networks should not be seriously degraded by security features. Therefore, the need exists to develop security architectures optimized for performance.

Remote Control System Vulnerabilities. Remote control systems (such as SCADA systems) provide distant control for distributed components within the communications industry and other infrastructures. The protection and security of these systems and protocols are critical for all infrastructures. Using real-time process control of systems over the Internet is an R&D issue.

Goals and Challenges

The goals and challenges are to develop tools and methodologies to efficiently, cost-effectively, design and implement new and improved security architectures.

Rationale for the Research and Desired Results

The rationale for the research is that the threat environment for the ICI is rapidly evolving, and new security technologies and concepts must keep pace with them. It is necessary to improve the focus on the fundamental research and proper design of security engineering and technology for architectures, which is introduced early in the development process to assure security in complex, distributed, multicomponent systems in a dynamic environment.

Timeframe and Resource Requirements

The timeframe for this activity extends at least to 2010. The total estimated investment over this period is $525 million. The proposed commitment is $125 million in 2000, $150 million between 2001 and 2005, and $250 million between 2006 and 2010.

3.3.2 Assurance Technologies

Description

The development of assurance technologies is a critical, long-term research area requiring government investment. The commercial sector rarely invests in this area because of the length of time to see a return on their investments. This topic involves the development of tools and techniques for rigorous design, implementation, testing, and formal verification of hardware and software components and their subsequent integration into larger systems. This research topic would focus on how to make assurance a normal component of system development, how to perform efficient product evaluation from a security perspective, how to do system-level assurance evaluations, how to develop statistical process control procedures, and how to use tools and methodologies for identification and authentication.

Making Assurance a Normal Component of System Development. System engineering teams and their engineering processes must be bolstered to make rigorous assurance methods a natural component of hardware and software engineering. Engineers need better design analogies and better integration concepts that support assurance justification. Technologies and methodologies that can provide this need include the following:

- Development of rigorous design languages that allow the formal expression of a concept or behavior;

- Development of formal protocol specifications and methods;
- Modeling and simulation tools; and
- Formal inspection, testing, model-checking, and verification procedures.

Efficient Product Evaluation Policies. The Trusted Product Evaluation Paradigm[9] used by DoD for two decades is no longer realistic. Although the intent was to evaluate a product once and then reuse the assurance evidence to certify many different system implementations, the actual results have not proven to be as effective as intended. Most product providers believe that continuing to evaluate a single product is irrelevant today because that product often must be adapted to work as part of a larger system.

System-level Assurance Evaluation. The current product evaluation approach does not give adequate support assurance at the system level. Procedures and tools need to be developed that address the following:

- Determining objectively what a product does in a process that is highly repeatable and relatively impervious to a different interpretation,
- Performing testing to assess security functionality,
- Providing a basis for characterizing security and system behavioral properties,
- Providing an understanding of the security contributions of various components and how to compose them, and
- Providing an understanding of the "weakest link" within the system at the component level.

Development of Statistical Process Control Procedures. Research is needed on applying statistical process control and other quality approaches to software and hardware engineering processes. Methods for effecting and measuring continuous process improvement through both quality and activity cost measures should be developed.

Identification and Authentication. One way to reduce threat is to limit access (physical or cyber) to critical and vulnerable components. As a result, technologies need further development. These technologies include biometrics and other methods for secure identification and authentication.

---

9 The Trusted Product Paradigm is built on four fundamental blocks: (1) security policy (access control), (2) accountability (identification and authentication and audit), (3) assurance (operational and life cycle), and (4) documentation. Such trust has been oriented largely toward the operating system and its Trusted Computing Base (DoD 1985).

Goals and Challenges

The goals and challenges are to develop tools and methodologies for efficient, cost-effective, implementation of new and improved assurance technologies. The effectiveness of the research should be demonstrated in large-scale studies using real systems.

Rationale for the Research and Desired Results

The rationale for the research is that breaks and disruptions in the ICI can be extensive and potentially life-threatening. Rigorous assurance methods, engineering, and evaluation strategies need to be developed and incorporated into system designs to assure the appropriate security functionality in multicomponent, integrated systems.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010. The total estimated investment over this period is $375 million. The proposed commitment is $95 million in 2000, $105 million between 2001 and 2005, and $175 million between 2006 and 2010.

3.3.3 Advanced Concepts and Theory

Description

The objectives of this research are to perform fundamental analyses into the complexities of advanced ICI systems and networks and the processes required to produce secure products, especially software. Examples of areas requiring study under this topic include the theory of protection, how to use expert systems for network management; understanding system-level hazards, tools, and methodologies for improving the quality of software; self-describing systems; and the security implications of systems of integrated components.

Theory of Protection. A theoretical basis through fundamental research is needed to protect the communications and information infrastructure. The security and protection implications of advanced communications concepts should also be studied. Analysis of this topic would result in a body of knowledge with a sound basis in academic research in protection technology.

Use of Expert Systems for Network Management. Advanced, expert-system-based software tools need to be developed for managing and administering complex networks. These tools would facilitate visualization and debugging of underperforming or overloaded networks, offer help in reconfiguring the network, and assist in evaluating hypothetical network architectures.

Understanding System-level Hazards. Innovative approaches are needed to improve our ability to understand system-level hazards, as well as to understand the individual and integrative risk contributions introduced by all system components, especially software.

Improving Software Quality. Theoretical work is required to determine ways in which to improve software quality and develop "safe" programs. This work would include the following:

- Development and use of CASE tools,
- Development of quality standards,
- Development of fault- or bug-tolerant software,
- Development of mathematically rigorous and formal methods,
- Use of standard development procedures, and
- Reuse of software.

Self-describing Systems. Research is needed to investigate techniques by which large-scale systems might "describe themselves" to modeling and analysis tools, to provide greater assurance that analysis of such tools is descriptive of large systems as actually constituted.

Systems of Integrated Components. Research is required on systems with many integrated components. This research would embrace such issues as composition of trustworthy systems from less trustworthy components, graceful degradation when breaks occur, and fine-grain damage containment.

Goals and Challenges

The goals and challenges are to develop the advanced concepts, theories, and tools needed to develop efficient and cost-effective security and protection for the ICI.

Rationale for the Research and Desired Results

The rationale for this research is that as technologies evolve and develop, new potential threats and vulnerabilities may emerge that require advanced concepts and theory to detect and protect against them. Further development of system theory and fundamentals is required to provide a comprehensive understanding of complex systems, at a theoretical and applied level, which is achievable through long-term research programs.

Timeframe and Resource Requirements

The timeframe for this activity extends at least to 2010. The total estimated investment over this period is $110 million. The proposed commitment plan is $30 million in 2000, $30 million between 2001 and 2005, and $50 million between 2006 and 2010.

3.3.4 Management of Information Protection

Description

The objective of this research is to develop methodologies and tools for the application and management of information protection in information and communications systems. Specific areas of study include how to protect data that exist on multiple nodes, how to protect information in a multiple-security-level environment, security based on advanced information protection concepts, the security and management implications of long-term information storage, and configuration management.

Protecting Data on Multiple Nodes. Techniques are needed to protect data in individual files as they reside on multiple nodes in a system. Individual repositories are not adequately protected. Thus, these files may need be encrypted, which means that methods are required to manage the keys for encrypting the files. These methods must support flexible, distributed authorization models, rather than manual key distribution.

Protecting information in wireless communication systems includes the confidentiality of location, levels of protection while roaming in the United States and foreign networks abroad, information security, and personal information on users.

Information Protection in a Multiple-security-level Environment. Metrics are needed for evaluating information protection when different tools and measures are combined in the security infrastructure.

Security Based on Advanced Information Protection Concepts. Security architectures must be developed that incorporate advanced information protection concepts, such as information that carries its own use conditions. (That is, the information may contain, for example, the categories of users that can access these data and the conditions under which they may do so.)

Long-term Information Storage. Research is needed to address the protection issues in long-term information protection. Data storage techniques and media have changed dramatically and are expected to continue to change. Stored media deteriorate with time, and recording protocols change. Research is required to ensure that knowledge about storage techniques is preserved so that data can be retrieved even if the method of storage has become obsolete. While this topic is not solely related to security, it is likely

to be a significant security issue, especially as storage and encryption technologies continue to advance.

Configuration Management. Research is required to improve methods for managing remote and local configuration. Errors in configuration management frequently lead to significant vulnerabilities that can be exploited. The next generation of wireless services is expected to permit the handset to be reconfigured by downloading appropriate software, and this capability requires appropriate security mechanisms and configuration control.

Goals and Challenges

The goals and challenges are to develop tools and methodologies for protecting information over time and in diverse environments.

Rationale for the Research and Desired Results

Information collection, analysis, and use are key elements in modern society. Damage or disruption to the information bases used by society could have dramatic consequences. The protection of information depends on the environment (e.g., multiple nodes, multiple security levels) and requires different tools and technologies. Research is needed to define and provide protection mechanisms for information in various system and network environments.

Timeframe and Resource Requirements

The timeframe for this activity extends at least to 2010. The total estimated investment over this period is $110 million. The proposed commitment is $10 million in 2000, $50 million between 2001 and 2005, and $50 million between 2006 and 2010.

3.3.5 Characterization of Minimum Infrastructure for Essential Services

Description

The objective of this research is to determine the minimum infrastructure components required to provide essential national, governmental, and military communication and information services. The characterization of these services includes assuring the exchange of information between government agencies and local authorities, maintaining the functionality of emergency management communication systems, and assuring redundant systems in critical areas.

Goals and Challenges

The goals and challenges are to identify the key elements of the ICI that require maximum protection in order to provide essential services.

Rationale for the Research and Desired Results

Loss or disruption of the ICI could result in serious and potentially dangerous consequences with respect to the continued operation of critical government and military services.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010. The total estimated investment over this period is $55 million. The proposed commitment is $15 million in 2000, $15 million between 2001 and 2005, and $25 million between 2006 and 2010.

3.3.6 Encryption Technology

Description

The objective of this research is to develop and evaluate software, firmware, and hardware encryption technologies. Specific areas of study include developing standards for security key management and providing affordable cryptography.

Standards for Security Key Management. Research is needed to develop a nationwide standard for security key management, including key discovery, key registration and dissemination, dynamic revocation, key refresh, and key escrow (as desired). The approach can use public key mechanisms, but the basic keys also should be suitable for symmetric use. The deployment and management of large public key infrastructures and symmetric key management are research issues that need resolution, in that this technology may form the common denominator in our distributed systems.

Affordable Cryptography. Research into applied cryptographic technology for privacy, integrity, authentication, nonrepudiation, etc., is needed. The emphasis should be on low-cost scalability, user-friendliness, and minimal overhead.

Goals and Challenges

The goals and challenges are to develop robust, high-performance, efficient, and cost-effective encryption technologies. Research needs include improved commercially available encryption technologies, high-speed cryptography for the national infrastructure, and cryptography for ultra-high-speed authentication and other applications.

Rationale for the Research and Desired Results

The rationale for this topic is that the potential effects of not being able to provide adequate protection of information are immense. The increased computer power now available to intruders necessitates the development of more robust and secure encryption technologies. However, the effective use of more robust algorithms requires the development of high-performance methods that can encrypt data more securely without inordinate increases in computation time.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least to 2010. The total estimated investment over this period is $525 million. The proposed commitment is $125 million in 2000, $150 million between 2001 and 2005, and $250 million between 2006 and 2010.

3.4 Modeling and Simulation Tools

Description

The requirement for this research affects all three primary areas because modeling and simulation tools are required in each of them. These tools are needed at the national level to assess risk, security, interoperability, and recovery issues. Examples of areas of study include the development of advanced simulation frameworks for testing and evaluation, the modeling of complex systems, and the modeling of system architectures.

Development of Advanced Simulation Frameworks. A general need exists for advanced simulation frameworks to support the analyses required in each area. For example, a need has been expressed to develop tools that can identify and map the vulnerabilities and interdependencies in systems and networks.

Modeling of Complex Systems. Fundamental work on modeling of complex systems is required. Understanding is limited concerning the components in an infrastructure, their performance implications, and their interaction with other components.

Modeling of System Architectures. Rigorous modeling and analysis at the systems architecture level is needed, and this modeling needs to be combined with techniques for tracking compliance of deployed systems with the architectural descriptions on which the analysis results are based. The need for architectural analysis techniques is well understood, and work is under way to adapt (to the infrastructure protection domain) such techniques as probabilistic risk assessment by means of fault-tree analysis.

Perhaps less well recognized is the problem of validating the results of such analyses in the presence of possible (likely) divergences of modeled systems from their

architectural models, especially in system evolution. In real industrial systems, this evolution occurs somewhat haphazardly and, for efficiency, sometimes without adequate, centralized control. The development of advanced modeling and simulation tools and environments would provide synthetic test beds for experimental studies of the infrastructure that cannot be performed under actual conditions.

Goals and Challenges

The goals are to develop the modeling and simulation tools necessary to create and evaluate the technologies required to protect the ICI. These models include the effects of specific attack elements and safeguards against those attacks.

Rationale for the Research and Desired Results

Modeling and simulation activity is a cost-effective way to research issues in a virtual environment on a computer without performing experiments on actual systems.

Timeframe and Resource Requirements

The timeframe for this activity extends to at least 2010 and perhaps beyond. The total estimated investment over this period is $535 million. The proposed commitment is $135 million in 2000, $150 million between 2000 and 2005, and $250 million between 2006 and 2010.

Section 4
R&D Topic Roadmaps

Table C.1 provides a summary of the research topics in each of the thrust areas, as well as in the crosscutting topic on modeling and simulation. Included are the type of research that would be performed, a description of the products that could be expected, the goals and challenges in each area, the performance goals and technical challenges, and a prioritization of the topics.

4.1 Roadmap for Development

Table C.2 provides a "roadmap" for the individual research areas and crosscutting modeling and simulation. The roadmap describes the research path to be followed, estimates of what could be expected over the timeframe 2000–2010, and the total estimated investment required. Table C.3 summarizes the recommended investments over all of the areas.

4.2 Suggested Pilot Projects

A number of pilot projects are recommended for demonstrating that enhanced security and protections can be provided in the information and communications infrastructure. Pilot projects would be used explicitly to refine requirements, apply research products in limited test environments (i.e., test beds), and provide valuable feedback to researchers. The recommended pilot projects are described in the following subsections.

4.2.1 Development of an Experimental Test Bed

It is recommended that an experimental test bed be developed for use in evaluating security technologies. This test bed would be government-funded but available to private-sector firms to test security technologies and interoperability issues.

4.2.2 Lexicon and Procedures for Defining and Reporting Data

A common set of definitions should be developed to describe threats, vulnerabilities, and types of attacks. This lexicon would enable researchers to collect data on threats, vulnerabilities, and attacks in a self-consistent manner so trends could be assessed. It is recommended that a system similar to one implemented by the FBI for reporting crime statistics be used.

Table C.1 Summary of R&D Topics for Information and Communications

Research Topic No.	Research Topic Title (Type[a])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category[b]
		Risks, Threats, and Vulnerabilities			
1	Vulnerability Detection and Analysis (B, A, ATD)	Information, management procedures, software tools, advances in fundamental theory	Provide efficient and effective tools to detect and analyze vulnerabilities	Physical, cyber, interdependencies	Most important
2	Valuation of Information (B, A)	Management procedures, software tools, advances in fundamental theory	Provide efficient, easy-to-use tools and procedures for valuing information	Physical, cyber, interdependencies	Very important
3	Risk Analysis (B, A)	Management procedures, software tools, advances in fundamental theory	Provide automated and effective tools for analyzing risk in systems	Physical, cyber, interdependencies	Important
4	Characterization and Notification of Threats (B, A)	Information, management procedures, advances in fundamental theory	Provide efficient and effective tools to collect, analyze, and disseminate data on threats	Physical, cyber, interdependencies	Most important
		Incident Detection, Response, and Recovery			
5	Intrusion and Incident Detection and Warning (B, A, ATD)	Information, management procedures, software and hardware technologies, advances in fundamental theory	Develop efficient, cost-effective tools and methodologies for rapid incident detection and warning	Physical, cyber, interdependencies	Most important
6	Response, Recovery, and Reconstitution (B, A, ATD)	Software and hardware technologies, management procedures, advances in fundamental theory	Provide rapid and efficient response, recovery, and reconstitution in the event of a break in service	Physical, cyber, interdependencies	Most important
		Engineering High-confidence Infrastructures			
7	Security Architectures (B, A, ATD)	Hardware and software technologies, management procedures, advances in fundamental theory	Develop efficient, cost-effective tools and methodologies, implement new and improved security architectures	Physical, cyber, interdependencies	Most important

Table C.1 (Cont.)

Research Topic No.	Title (Type[a])	Product	Goals and Challenges	Threats and Vulnerabilities	Priority Category[b]
Engineering High-confidence Infrastructures (Cont.)					
8	Assurance Technologies (B, A, ATD)	Hardware and software technologies, management procedures, advances in fundamental theory	Develop efficient, cost-effective tools and methodologies, implement new and improved assurance technologies	Physical, cyber, interdependencies	Most important
9	Advanced Concepts and Theory (B, A, ATD)	Hardware and software technologies, advances in fundamental theory	Develop the advanced concepts and tools needed to provide efficient and cost-effective security and protection	Physical, cyber, interdependencies	Very important
10	Management of Information Protection (B, A, ATD)	Hardware and software technologies, management procedures	Provide tools and methodologies for the effective application and management of information protection	Physical, cyber, interdependencies	Most important
11	Characterization of Minimum Infrastructure for Essential Services (A, ATD)	Information, hardware and software technologies, management procedures	Identify the key elements in the ICI that must be given maximum protection to provide essential national, governmental, and military ICI services	Physical, cyber, interdependencies	Very important
12	Encryption Technology (B, A, ATD)	Hardware and software technologies, management procedures	Develop effective and affordable encryption technologies	Physical, cyber, interdependencies	Important
Modeling and Simulation Tools for Infrastructure Protection					
13	Modeling and Simulation Tools (B, A, ATD)	Software technologies, advances in fundamental theory	Develop tools and methodologies for simulating complex systems and analyzing different system architectural constructs	Physical, cyber, interdependencies	Very important

[a] B = basic; A = applied; ATD = advanced technology development; and POP = proof of principle and validation.

[b] The order of the R&D topics within a priority category (most important, very important, and important) does not imply relative importance.

Table C.2 Summary of Information and Communications R&D Roadmap

R&D Topic No.	Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimate[a])	Achieved by ~2010 (Resource Estimate[a])
		Risks, Threats, and Vulnerabilities		
1	Vulnerability Detection and Analysis	Develop procedures for collecting, analyzing, and disseminating vulnerability information. ($90 million)	Develop lexicon and database to identify vulnerability information about the infrastructure. Develop metrics and measures to gauge the effectiveness of tools to detect and analyze vulnerabilities, and automate tools to detect vulnerabilities. ($90 million)	Develop coordinated and scalable tools for vulnerability detection and data notification at the national level. Establish international cooperation for collecting and sharing information on vulnerabilities. ($150 million)
2	Valuation of Information	Develop manual tools, techniques, and procedures to assess the value of information. ($30 million)	Develop automated tools to assist information owners in assessing the value of information and determining appropriate levels of protection. ($30 million)	Develop and refine automated tools to assist information owners in assessing the value of information and protection, including information that can be aggregated from multiple sources. ($50 million)
3	Risk Analysis	Develop semiautomated risk analysis tools and formulate techniques and metrics to assess risk. ($75 million)	Develop automated risk analysis tools to dynamically assess risk on systems and networks as components change. ($75 million)	Develop advanced and automated risk analysis tools to incorporate the emergence of new technologies and system components. ($50 million)
4	Characterization and Notification of Threats	Develop procedures for collecting, analyzing, and disseminating threat data. ($25 million)	Implement national database of threat and response information. Profile potential attackers. ($30 million)	Develop and distribute coordinated, national-level tools for threat notification. Establish international cooperation for collecting and sharing threat data. ($40 million)

Table C.2 (Cont.)

R&D Topic No.	Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimate[a])	Achieved by ~2010 (Resource Estimate[a])
		Intrusion and Incident Detection, Response, and Recovery		
5	Intrusion and Incident Detection and Warning	Develop manual tools and procedures to detect incidents and issue warnings. Establish metrics for assessing intrusion detection systems. ($90 million)	Develop automated tools to detect incidents and issue warnings, strategy-based intrusion detection systems, automated trace-back tools, and scalable detection systems. ($90 million)	Develop scalable tools at a national level to detect indications and warnings of an attack. Establish international cooperation and sharing of data on attacks. Create scalable assessment tools to evaluate Internet threats. ($150 million)
6	Response, Recovery, and Reconstitution	Develop manual tools to detect, contain, and eject intruders, and to perform triage for recovery on attacked systems. ($95 million)	Develop automated tools to detect, contain, and eject intruders, and perform triage for recovery on attacked systems. ($105 million)	Continue development of automated tools to improve robustness, efficiency, and timely response in recovery. ($100 million)
		Engineering High-confidence Infrastructures		
7	Security Architectures	Establish methodologies for automated distribution of security patches. Prepare security implementation policies. ($125 million)	Develop advanced firewall technologies and active, dynamic network technologies. ($150 million)	Develop scalable, robust security architectures to integrate security components. ($250 million)
8	Assurance Technologies	Establish standards and methods of incorporating assurance into system development and complete product evaluation policies. ($95 million)	Develop tools for efficient product evaluation and system-level evaluations. ($105 million)	Continuously develop and refine methodologies and techniques for incorporating assurance into system development. ($175 million)
9	Advanced Concepts and Theory	Establish standards, techniques, and procedures for software development. ($30 million)	Research and develop ways to use expert systems in network management and to adaptively secure systems. ($30 million)	Develop self-describing secure systems. ($50 million)
10	Management of Information Protection	Research and develop concepts and techniques for protecting data and performing configuration management in local and remote infrastructure components. Define performance metrics for evaluating information protection. ($30 million)	Research information protection concepts that carry use conditions, or metadata, with the information. Establish economic metrics for evaluating information protection. ($30 million)	Continuously develop and refine measurement concepts, tools, and technologies for managing the protection of data in diverse environments. ($50 million)

Table C.2 (Cont.)

R&D Topic No.	Title	Near Term (Resource Estimate[a])	Achieved by ~2005 (Resource Estimate[a])	Achieved by ~2010 (Resource Estimate[a])
Engineering High-confidence Infrastructures (Cont.)				
11	Characterization of Minimum Infrastructure for Essential Services	Define and characterize minimum essential government and military communications, operations and services, and the required infrastructure to support those services. ($15 million)	Establish interagency contingency and coordination plans and address the introduction of redundant systems in critical applications. ($15 million)	Develop plans and deploy additional technologies to ensure redundancy as new technologies emerge and the scope of government services evolves. ($25 million)
12	Encryption Technology	Establish national standards for security key management. ($125 million)	Develop robust, high-performance, cost-effective cryptographic technologies. ($150 million)	Continually advance and refine robust encryption technologies given the significant increases in computing power available. ($250 million)
Modeling and Simulation Tools for Infrastructure				
13	Modeling and Simulation Tools	Define requirements and initiate modeling and simulation on small network systems. ($135 million)	Develop tools and models for modeling complex systems at the architectural level, and tools and techniques for modeling inter-dependencies and vulnerabilities in systems. ($150 million)	Develop automated tools for detecting deviations from system specifications at the architectural level, and technologies and specifications for self-describing systems. ($250 million)

[a] Resource estimates reflect qualitative, order-of-magnitude judgments. They are intended to be representative of the resources needed for the R&D topics and are based on assumptions concerning the scope, the expected level of effort, and the pace of the research. Detailed cost estimates must be prepared in concert with the development of detailed R&D plans.

Table C.3 Summary of Estimated Research Investments for Enhancing the Protection of the ICI (in millions of U.S. dollars)

Area and R&D Topic	Year 2000	~ 2001 – 2005	~ 2006 – 2010[a]	Total
Risks, Threats, and Vulnerabilities	**70**	**375.0**	**290.0**	**735.5**
Characterization and Notification of Threats	5	50	40	95
Vulnerability Detection and Analysis	30	150	150	330
Valuation of Information	10	50	50	110
Risk Analysis	25	125	50	200
Intrusion and Incident Detection, Response, and Recovery	**55**	**325**	**250**	**630**
Intruder and Incident Detection and Warning	30	150	150	330
Response, Recovery, and Reconstitution	25	175	100	300
Engineering High-confidence Infrastructures	**100**	**800**	**800**	**1,700**
Security Architectures	25	250	250	525
Assurance Technologies	25	175	175	375
Advanced Concepts and Theory	10	50	50	110
Management of Information Protection	10	50	50	110
Characterization of Infrastructure for Minimum Essential Services	5	25	25	55
Encryption Technology	25	250	250	525
Modeling and Simulation Tools for Infrastructure Protection	**35**	**250**	**250**	**535**
Totals	**260**	**1,750**	**1,590**	**3,600**

[a] The funding estimates given for the 2006 to 2010 timeframe will most likely change as a result of developments from 2001 to 2005.

Section 5
Complexities

The information and communications component of the infrastructure has unique characteristics and complexities not shared by the other infrastructures.

5.1 System Administrator and User Trust

Successful implementation of any security technologies and procedures ultimately depends on the persons who use the tools and procedures. Individual users must be trusted to protect passwords and follow established procedures. Select individuals must be trusted to manage keys and master passwords. Other trusted individuals or groups must be responsible for validating private/public key holders and certifying electronic identities. These individuals also require the proper training and tools to recognize and rectify security shortfalls (e.g., configuration issues) in the systems they control.

5.2 Threats and Vulnerabilities from an International Perspective

Attacks on the ICI can originate from anywhere in the world via computer connections and the Internet. Traditional international boundaries and checkpoints, and their associated protections, no longer apply. Systems become vulnerable from the interconnection of numerous networks, which are only as secure as the weakest link in the chain. Tools and technologies to assess, measure, and model the interconnection of complex components are needed, along with sharing of threat information on an international scale, as discussed earlier.

5.3 Readily Available Advanced Attack Tools

The tools available to hackers are becoming more sophisticated and are available through the World Wide Web. Many tools available for protecting systems also can be used to penetrate systems. The design of security products typically lags behind the technological capability of the hackers to penetrate systems. New laws and stricter enforcement of existing laws are required to increase the level of deterrence.

5.4 Security Priority

Security shortfalls may develop as a result of corporate downsizing, through initiatives to increase profitability in an increasingly competitive market, and through the breakup of large companies into smaller companies with fewer resources to spend on security. As a by-product of downsizing, many firms are outsourcing portions of their business. As a result, external consulting firms can access computer systems to obtain information necessary to perform their tasks. Guidance for influencing corporate policy in

the security area is required to maintain the security of systems and information in a changing corporate culture and environment.

Section 6
Other Important Issues

Other issues related to the protection of the ICI exist; although they are not R&D topics, they also affect the degree to which the ICI can be protected.

6.1 Education Curricula and University Funding

Developers need to include protection concepts routinely in the development process, and the place to start is the educational system. There is a requirement for enhanced academic education and for the diversification of research. Too few students are entering the field of communications and information protection, and too few academic institutions have relevant, high-quality research programs. More academic institutions should have curricula and degrees related to communications and information protection; this, in turn, would require support for course development and computing resources for students. Current research topics and objectives are too limited. It is important to foster creativity by ensuring that research groups and individual researchers are consistently funded. Government funding can be leveraged by requiring universities to develop robust curricula, faculty expertise, and their own research programs as the basis for continued funding.

6.2 Continuous Training for System Administration

As systems and technologies change, the administration of the systems will also evolve. Systems administrators require continuous training (as noted in Section 5.1) to keep up with the changes. Advanced, and automated, training systems are required.

6.3 Growth and Consolidation in the Security Industry

The computer security industry is experiencing strong growth. Projections show that the industry could grow from $2 billion in 1997 to almost $7 billion by 2000 (*International Herald Tribune* 1998). The computer and information security industry is experiencing the beginning of consolidation. Small, successful start-up programs are being acquired by larger companies, and the number of companies providing computer and information security is beginning to decrease. Whether the consolidation will lead to better products or to reduced competition and less diversity is question for debate.

6.4 Legal Issues

Legal questions related to liability must be resolved. For example, suppose an attack occurred on the communications and information infrastructure. What responses would be allowable, legal, and acceptable? Who would have legal jurisdiction to investigate or prosecute? This uncertainty over potential liabilities is probably one of the factors that has

limited the deployment of security infrastructures. This factor is of particular concern if a party is held liable for the actions or inactions of others.

Many legal issues arise when virtually any individual or group of individuals can visit our country electronically, without the protocol and checks and balances required for a physical visit. One solution to the jurisdiction issue could be to establish virtual borders that would enclose domains where certain rules and laws would apply.

Questions associated with privacy and anonymity also need to be addressed. Currently, data can be aggregated from multiple sources — Social Security and medical records and from other government files — to find information about individuals and businesses that, in the world of paper files, would be confidential. Furthermore, many modes of communication in our society provide anonymity, and people expect comparable capability from the infrastructure. Governments are currently working to define principles to ensure privacy, but implementation of these principles depends on effective security. The solution to the privacy question is complicated by the need to reconcile the means of protecting privacy with the technologies and policies related to detecting and responding to intrusion. Once legal and privacy issues are resolved, industry should be more willing to devote substantial R&D resources to areas once avoided because of fear of liability or litigation.

6.5 Information Sharing

To design and implement effective countermeasures, and to make competent decisions about the use of resources, the R&D community requires more information about vulnerabilities, threats, and incidents. Enhanced collection and timely dissemination of intelligence information (foreign and domestic) on the nature and extent of threats to the communications and information infrastructure are essential. Security classification and information-handling guidelines must be reassessed to maximize dissemination of threat and vulnerability information so that this information can be widely, though not necessarily openly, available. Many individuals who do not possess security clearances must have timely access to this information. Recently, the FBI established the National Infrastructure Protection Center to investigate cyber crime; this entity is a candidate for functioning as a liaison between multiple government agencies and private-sector firms.

6.6 Industry/Government Partnership

An industry/government partnership is needed to track R&D milestones, which would provide a continuous assessment process to continue the roadmap set forth here. This government outreach program is needed to continue to set research priorities, while tracking and monitoring the research initiatives under way, as well as to leverage and investigate diverse research areas, without duplication, into actual projects and pilots that can significantly improve infrastructure protection and security. A clearinghouse for research across industry and the government is needed. Issues of classified research and proprietary work need to be handled at some abstract level.

6.7 International Issues

The protection of the infrastructure has become an international issue because of the interconnection of networks and the Internet. The United States should initiate cooperation agreements and lead collaboration efforts to develop and enforce infrastructure protection measures. At the same time, care must be taken to develop key security software in the United States. Currently, many U.S.-produced consumer software products have security technologies produced by contractors in Finland, Australia, Germany, and Russia. U.S. policies and laws, including a reasonable encryption policy, should support domestic production.

6.8 Year 2000 Software Update Initiative

The large volume of legacy code and the time deadline for avoiding potential failures make the year 2000 update initiative a significant challenge for the government and the private sector. The availability of resources to handle the new security initiatives may be considerably constrained in the near term because of the absolute necessity to deal with the year 2000 problem. For example, General Motors has estimated that it would cost between $360 million and $500 million to update its systems, while the Unilever Group has increased its estimate to £300 million (*Financial Times* 1998). An aspect of the year 2000 problem not often discussed is that even if the United States successfully converts all of its important software systems, failures on the international level may result in problems in this country.

6.9 Cryptography

Cryptography policy is an issue that is beyond the scope of this R&D study. However, it is recognized that research into applied cryptographic technology for privacy, integrity, authentication, nonrepudiation, and other critical areas is essential for effective infrastructure assurance. The mathematical algorithms used to encrypt data must be highly resistant to attack and computationally secure. The keys used for encrypting and decrypting data must be distributed properly, protected, and managed. Promising new encryption technologies, such as elliptic curve, could improve both security and economy of operations. In addition, new concepts of key management infrastructure could emerge to provide a variety of alternatives that industry could develop into interoperable products.

Section 7
References

Defense News, 1998, "Clinton Prepares Infowar Response," Vol. 13, No. 11, March 16–22.

Financial Times, 1998, April 4–5, p. 6.

International Herald Tribune, 1998, March.

Internet Week, 1998, "Burned by Your Firewall?" March 30, p. 9.

Mayfield, T., 1998, *Critical Infrastructure Protection: An Academic & Institution Perspective on Research & Development for the Information & Communications Infrastructure*, Institute for Defense Analyses, April 15.

National Telecommunications and Information Agency (NTIA), 1996, *In the Matter of Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket No. 96-98, Reply Comments, U.S. Department of Commerce, Washington, D.C., May 30.

Q.V., 1995–1996, e.g.: 220 ILCS (Illinois) 5/13-102; *Implementing the Telecommunications Act '96*, Washington Utilities and Transportation Commission, summary of Report Findings, November 30, 1996; California Public Utilities Code, Chapter 4, Article 8, Pars. 851–856 (Universal Service); New Jersey Board of Public Utilities, Ratepayer Advocate Recommendations, Section V. *Definition of Universal Service*; and, Public Utility Commission of Texas, Rule ¶23.97, related to interconnection for local exchange service, Report of the Commission, references to universal, nondiscriminatory service as defined by the U.S. Telecommunications Act of 1996; Texas Register (20 TexReg 8777), October 24, 1995.

The Washington Post, 1998, "Panel Urges U.S. to Power Up Cyber Security," March 20.

U.S. Department of Defense (DoD), 1985, TCSEC, DoD 5200.28-STD.